[Insert Cover Picture]

Indoor Performing Arts / Theater Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 9:00 a.m. | Welcome and Participant Briefing |
| 9:00 a.m. | 9:50 a.m. | Module One: Intelligence and Information Sharing |
| 9:50 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 10:50 a.m. | Module Two: Incident Response |
| 10:50 a.m. | 11:00 a.m. | Break |
| 11:00 a.m. | 12:00 p.m. | Module Three: Recover and Business Continuity |
| 12:00 p.m. | 12:30 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Indoor Performing Arts / Theater Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] at [insert exercise location]. Exercise play is limited to [insert exercise parameters].  This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [Select applicable Mission Areas] |
| **Capabilities** | * Community Resilience * Economic Recovery * Healthcare and Emergency Medical Services (EMS) * Intelligence and Information Sharing * On-Scene Security and Law Enforcement * Operational Communications * Operational Coordination * Planning * Public Health * Public Information and Warning * [Insert additional core capabilities as necessary] |
| **Objectives** | 1. Examine pre-incident and incident information sharing procedures between public and private sector partners. 2. Examine emergency response, evacuation, and shelter-in-place plans and procedure to a complex coordinated attack. 3. Examine recovery and business continuity plans following a complex coordinated attack. 4. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Vehicle ramming incident with an active shooter. |
| **Scenario** | The TTX will focus on pre-incident information sharing and response to and recovery from a complex coordinated attack. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine pre-incident and incident information sharing procedures between public and private sector partners. | * Intelligence and Information Sharing * Planning * Public Information and Warning |
| Examine emergency response, evacuation, and shelter-in-place plans and procedures to a complex coordinated attack. | * On-Scene Security and Law Enforcement * Operational Communications * Operational Coordination * Public Health, Healthcare, and EMS |
| Examine recovery and business continuity plans following a complex coordinated attack. | * Community Resilience * Economic Recovery * Public Information and Warning |
| [Insert additional objectives, as necessary.] | * [Insert additional core capabilities, as necessary.] |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Date Collectors** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Intelligence and Information Sharing
* Module Two: Incident Response
* Module Three: Recovery and Business Continuity

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Intelligence and Information Sharing

## Scenario

## [Insert Location: Insert Facility Name and Location]

### [Insert Month, Day, Year]

There has been a vehicle-borne improvised explosive device (VBIED) attack at the [insert foreign performing arts center] in [insert foreign city]. This resulted in the injuring and killing of dozens of visitors who were waiting to attend a highly popular theater production. Some extremist groups decry some of the messages of said production.

A group known as [insert organization] has claimed responsibility for the attack, citing it as an initial call to action against any organizations that intend to provoke or offend the public through public displays that “cross the line of standards and good taste.” [Insert organization] has also released several communiques calling upon “their brothers and sisters in arms” to conduct similar attacks at similar venues or other places of large gatherings. [Insert organization] is a known terrorist organization that advocates for a violent uprising against what they consider moral corruption.

International law enforcement agencies have located at least one social media site that has several references to an explosion in [insert your city] and have found many comments sympathizing with the performing arts center attacker. Based on comments within the online postings, investigators suspect that one of the attack “sympathizers” may be a former employee who has knowledge of inner [insert performing arts center] workings and is using software to hide their specific Internet Protocol address and location.

## Discussion Questions

1. What do private sector stakeholders expect from the federal government and intelligence community at this time?
2. How will your organization receive this information?
3. How long does it take for your organization to process information for sharing?
4. What security measures, if any, will private sector stakeholders employ following this incident?
5. How does your organization engage local law enforcement?
   1. Have you shared your emergency response plan with local first responders?
   2. Have local first responders visited your facility to gain familiarity with the site?
6. What actions are local, state, and federal law enforcement agencies taking at this point?
7. What security recommendations, if any, are local, state, and federal law enforcement making to private sector stakeholders at this time?
8. How does your agency or organization triage the information you receive (formal reporting, hearsay, social media, etc.)?
9. How would your agency or organization expect to receive information about a credible threat?
10. What steps does your organization take once they receive notice of a credible threat?
11. Are there additional notifications that your organization needs to make outside of your organization?
12. What plans exist describing the required protective measures your organization needs to take?
13. Who is in charge of engaging the public about the elevated threat level?
14. Does your organization communicate this information to the public and, if so, how?
15. Does your agency or organization conduct any specific training based on credible threats?
16. Does this training include emergency management or active shooter elements?
17. Can local law enforcement provide active shooter training for your organization?
18. Does this training include the Incident Command System (ICS)?
19. Would your actions change if the threat were specific to performing arts centers in the central United States?

# Module Two: Incident Response

## Scenario

## Location: [Insert Facility Name and Location]

### [Insert Month, Day, Year]: [Time]

It is a calm evening at the [insert your organization’s performing art center] and a sellout crowd is lining up outside the facilityfor opening night of a popular production. As people begin to enter the building, a van traveling south on [insert street] at a high speed accelerates into the line of patrons entering through the [insert center entrance].

The vehicle injures many people as it rams its way through the waiting line and crashes into the side of the building. As the vehicle comes to a stop, a single individual exits the vehicle with a handgun and begins firing indiscriminately into the crowd. The entrance of the [insert performing arts center] fills with frightened visitors attempting to escape the gunfire.

In addition to the victims of the vehicle ramming and gunfire, many people suffer injuries from panicked individuals scrambling over and around each other looking for safety. An off**-**duty [insert city/county] police officer who was attending the event confronts the shooter and neutralizes the individual.

As 911 calls flood in, a sweep of the area concludes the attacks killed or injured over [insert number causalities] individuals. Law enforcement cannot determine an exact number of fatalities at this time. Fire, EMS, and law enforcement personnel begin to secure the scene and attempt to triage the dead and wounded.

## Discussion Questions

1. What is the standing security posture at your facility prior to an event?
   1. What level of security / law enforcement would be on-site that could effectively respond to this type of attack?
   2. How does your organization train security personnel to respond to this type of attack?
   3. Do local law enforcement and venue security conduct cross-training?
   4. If so, does the cross-training cover complex coordinated attacks?
2. What standard operating procedures (SOPs) do officers take when arriving / making entry into the [insert performing art center] during an incident?
3. What steps must responders take prior to engaging the shooter?
4. Who is responsible for securing the scene?
5. What protocols exist to allow fire and EMS personnel to enter the [insert performing art center] to aid injured customers and casualties?
6. Are there established protocols at [insert performing art center] to alert visitors and employees to an emergency?
   1. Who is responsible for enacting these protocols?
7. Does [insert performing art center] train employees to respond to a dynamic incident such as this?
   1. Do your SOPs include roles and responsibilities for employees in the event of an incident such as this?
8. How quickly is your organization releasing messages to the public?
   1. Who is responsible for this type of messaging?
   2. How is your organization releasing this messaging?

**Scenario Update**

## Location: [Insert Facility Name and Location]

**[Insert Month, Day, Year]: [Incident Time + 45 minutes]**

Forty-five minutes have passed since the attack at [insert performing art center], and police officials are clearing the area and setting up a perimeter for the investigation.

First responders have established Incident Command, identified warm zones for triage, and are continuing to transport victims to local hospitals.

Responders evacuated all visitors that were in the building, and additional law enforcement have arrived on-scene to begin secondary sweeps. Law enforcement officers pry open the shooter’s crashed vehicle and discover what is believed to be an improvised explosive device (IED).

**Discussion Questions**

1. What type of command structure would responders establish?
   1. Who would be in charge?
   2. How does your organization represent itself within the ICS / Unified Command System?
2. Do different agencies or organizations cross-train on this type of incident? If so, what organizations involve themselves?
3. What additional law enforcement assets are available for your organization to request?
   1. What would their response time be?
   2. How would the response change following the IED identification by law enforcement?
   3. What additional agencies or resources would responders need to address an IED threat?
   4. What law enforcement SOPs might affect other organizations involved in or impacted by response operations (i.e., relocating fire and EMS responders out of an IED blast radius after discovering the explosive, etc.)?
4. At what point would responders contact federal authorities?
5. Would there be on-site EMS personnel working with local EMS? Who is in charge?
6. How would your organization coordinate an evacuation or shelter-in-place of [insert performing art center] occupants?
   1. What agency will take the lead in this endeavor?
      1. How do responders share this plan with [insert performing art center] occupants and guests?
7. Does the [insert performing art center] conduct an accountability check of their employees or independent vendors?
8. What steps need to take place to ensure your organization clears the [insert performing art center] of all gunmen?
9. What communication takes place with or between [insert performing art center] officials?
10. What communication platforms does [insert performing art center] use to communicate with employees?
11. How does your organization alert surrounding organizations or businesses to the incident?
    1. Who is responsible for this communication?
    2. Do your organization’s SOPs outline this process?
12. What information, if any, would your organization pass on to the public?
    1. How quickly does your organization notify the public of the incident?
    2. Who is in charge of this messaging?
    3. How do different agencies and organizations coordinate this messaging?
    4. Has your public information office had the opportunity to work with other agencies’ and organization’s public information personnel?
    5. Does your organization have “canned” or predetermined incident notifications that cover this type of incident?
13. Are there social media resources available during and immediately after an incident?
14. What measures does your organization take to disrupt the distribution of fake or misleading information?

# Module Three: Recovery and Business Continuity

## Scenario

## Location: [Insert Facility Name and Location]

### [Insert Incident Date + 1 Day]

One day has passed since the attack**,** and police officials have determined that the active shooter was a former employee of the [insert performing arts center] who [insert performing arts center] fired for underperformance several months earlier. [Insert performing arts center] remains closed, as it is still part of an ongoing investigation.

So far, over [amount of people] [insert performing arts center] visitors were killed or injured in the attackor during the ensuing panic while attempting to flee the incident area.

As expected, social media is rampant with rumors and speculation about the incident. Some claim there were explosive devices inside the center, while others claim that there were multiple gunmen on the loose. Multiple news outlets continue to dispatch reporters to the scene to interview witnesses and capture footage of the area.

In addition, [insert performing arts center] and 911 call centers have received numerous requests for information about the incident from families and friends worried about loved ones.

## Discussion Questions

1. Does your organization have a continuity of operations plan? If so, does it include a crisis communications plan?
2. What communication takes place between [insert performing arts center] officials and first responders after the incident?
   1. What other agencies / organizations do you need to contact at this time?
3. What messaging does your organization send out to the occupants about the current situation?
   1. What information does your organization convey to the public at this time? And how?
4. Do you have comprehensive, established family assistance or reunification procedures to reunite loved ones efficiently?
   1. How quickly does your organization activate reunification procedures?
   2. Has your organization trained and / or tested these procedures?
5. Do you have a pre-identified reunification center for employees and visitors to reunite with loved ones?
6. If so, have you pre-communicated the reunification center with employees and other applicable stakeholders (e.g., through employee orientations or the organization’s website)?
7. With whom would you be coordinating to activate the reunification center?
8. If applicable, do you have existing agreements with other organizations to assist in providing resources or shelter?
9. How would you address crowd control and media control, including directing parking?
10. What mental health services are available for employees and responders?
11. What SOPs exist for assisting visitors the incident impacted?
12. How would your organization communicate available services?
13. How would your organization handle incoming requests for information over the phone?
14. What about requests coming through various social media sources?
15. How does the investigation affect other nearby locations?

**Scenario Update**

## Location: [Insert Facility Name and Location]

### [Insert Incident Date + 2 days]

Two days have passed. The law enforcement investigation continues, and [insert performing arts center] employees are still restricted from entering the facility. [Insert performing arts center] officials have begun the damage assessment process to determine the facility repair costs.

National and international news outlets continue to dispatch reporters to the scene to interview witnesses and capture footage of the area. Interview requests with employees and [insert performing arts center] officials inundate the [insert performing arts center].

**Discussion Questions**

1. What resources is your organization considering for short-term recovery assistance?
2. Does your facility have trauma or mental health counseling available to employees?
3. Does your facility provide counseling to visitors and / or vendors who were at the site of the incident?
4. Do your plans, policies, and procedures outline this?
5. Does your organization track participation to ensure outreach is successful?
6. What type of messaging will your organization send to employees? How will you send the messaging?
7. What training do employees receive regarding media relations and the release of sensitive information?
8. What are the priorities at your facility post-incident?
9. Do your plans, policies, or procedures specify these priorities?
10. How do you communicate these priorities internally?
11. Does your organization coordinate priorities with county emergency management?
12. Does your organization coordinate priorities with state or federal agencies?
13. How long will it be before your organization opens the impacted building(s) for use?
14. Will your organization only close the affected building(s), or the entire organization?
15. Are there established plans to manage donations after the incident? Who is responsible for this task?
16. Are there established plans to handle memorials after the incident? Who is responsible for this task?
17. What local, state, or federal resources are available to assist in recovery?
    1. Does your facility have memorandums of understanding (MOUs) with local response agencies or other performing arts organizations?

**Scenario Update**

## Location: [Insert Facility Name and Location]

### [Insert Incident Date + 30 days]

It has been 30 days since the attack. Internal and external repairs to the damage the vehicle crash and gunfire caused continue at the [insert performing arts center]. At least half of the [insert performing arts center] employees remain unavailable for work.

**Discussion Questions**

1. What is the financial impact on the [insert performing arts center] during the time it is closed?
   1. What is the financial impact on employees during the time the [insert performing arts center] is closed?
   2. What is the financial impact on the surrounding businesses?
2. At what point would you consider [insert performing arts center] and all associated organizations or businesses stabilized and back to steady state?
   1. Who determines when it is safe for visitors to return to [insert performing arts center]?
   2. How does your organization communicate that to the public?

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Services |
| **EPT** | Exercise Planning Team |
| **ICS** | Incident Command System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **MOU** | Memorandums of Understanding |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOPs** | Standard Operating Procedures |
| **TTX** | Tabletop Exercise |
| **VBIED** | Vehicle-Borne Improvised Explosive Device |

